Nationale Cybersecurity Strategie 2

Van bewust naar bekwaam



Voorwoord

Al meer dan twee decennia maakt het cyberdomein onderdeel uit van de Nederlandse maatschappij. In deze periode is informatie- en communicatietechnologie (ICT) een belangrijke factor gebleken voor productiviteitsgroei en innovatiekracht. Binnen Europa is Nederland leidend in de wijze waarop wordt ingespeeld op technologische trends en het effectief gebruik van ICT-middelen en -vaardigheden. Nederland is een internationaal internet-knooppunt, heeft de meest competitieve internetmarkt ter wereld en één van de hoogste online gebruikers-dichtheden.

Voor het functioneren van onze samenleving is het waarborgen van de digitale veiligheid en vrijheid en het behouden van een open en innovatief cyberdomein een randvoorwaarde. Daarom is in 2011 de eerste Nationale Cybersecurity Strategie (NCSS1) verschenen. Doel van de NCSS1 was om met een integrale cybersecurity-aanpak gebaseerd op publiek-private samenwerking een veilig, betrouwbaar en veerkrachtig digitaal domein te realiseren en de kansen te benutten die dit onze samenleving biedt.

De (internationale) ontwikkelingen in het cyberdomein gaan snel. Afgelopen jaren is de (potentiële) impact van cyberdreigingen door uiteenlopende incidenten steeds duidelijker geworden. Het gaat hierbij niet alleen om dreigingen die onze cyberinfrastructuur kunnen verstoren, maar ook om dreigingen ten aanzien van de integriteit, beschikbaarheid en vertrouwelijkheid van de informatie die wij digitaal vastleggen, analyseren en uitwisselen.

Om adequaat te kunnen blijven reageren, zal Nederland de komende jaren inzetten op het verder versterken en bundelen van de krachten van betrokken publieke en private partijen, zowel nationaal als internationaal. Daarbij is het belangrijk cybersecurity niet geïsoleerd te benaderen, maar nadrukkelijk te bezien in samenhang met mensenrechten, internetvrijheid, privacy, maatschappelijke groei en innovatie. De Nationale Cybersecurity Strategie 2 (NCSS2) zet deze bredere kabinetsvisie op cybersecurity uiteen en benoemt verantwoordelijkheden en concrete acties.

Bij de totstandkoming van deze nieuwe cybersecurity-strategie zijn circa 130 partijen (publieke en private



partijen, kennisinstellingen en maatschappelijke organisaties) betrokken en is nadrukkelijk de dialoog met de bredere ICT-community gevoerd. Op verzoek van het kabinet heeft daarnaast de Cyber Security Raad, bestaande uit vertegenwoordigers van publieke en private partijen en wetenschap, geadviseerd over de koers van de nieuwe strategie.

Met deze strategie wil Nederland internationaal leidend blijven op het gebied van cybersecurity. We beginnen niet op nul. Nederland heeft een sterke cyberinfrastructuur en kent vele internetpioniers en innovatieve ICT- ondernemers die wereldwijd actief zijn. Nederland heeft daarnaast een bewezen talent voor het bouwen van coalities: niet alleen nationaal, maar ook op het terrein van internationale vrede en veiligheid. Samen kunnen we een veilig, vrij en rendabel digitaal domein realiseren. Iedereen zal hierbij verantwoordelijkheid moeten nemen voor zijn eigen digitale weerbaarheid en die van de samenleving als geheel. Het kabinet neemt met deze nieuwe strategie het voortouw en zal jaarlijks rapporteren over de voortgang.

De minister van Veiligheid en Justitie,
I.W. Opstelten

Inhoudsopgave

We gaan van structuren naar coalities, waarin alle partijen zijn vertegenwoordigd, nationaal en internationaal. Zo komen we tot gedragen normen en standaarden.



Management-samenvatting

Al meer dan twee decennia maakt het cyberdomein[1] deel uit van de Nederlandse maatschappij en heeft het een belangrijke bijdrage geleverd aan productiviteitsgroei en innovatiekracht. Nederland heeft veel geïnvesteerd in de wijze waarop wordt ingespeeld op technologische trends en het effectief gebruik van ICT-middelen en -vaardigheden. Nederland is mede daardoor een internationaal internetknooppunt, heeft de meest competitieve internetmarkt en één van de hoogste online gebruikersdichtheden ter wereld. Het cyberdomein is dan ook steeds meer verweven met ons dagelijks leven. De veiligheid van het cyberdomein is randvoorwaardelijk voor het optimaal benutten van de kansen die digitalisering onze samenleving biedt.

> ***Cybersecurity*** *is het streven naar het voorkomen van schade door verstoring, uitval of misbruik van ICT en, indien er toch schade is ontstaan, het herstellen hiervan.*
>
> *De schade aan ICT kan bestaan uit aantasting van de betrouwbaarheid van ICT, beperking van de beschikbaarheid en schending van de vertrouwelijkheid en/of de integriteit van in ICT opgeslagen informatie.*

In de afgelopen jaren is meer zicht gekomen op de dreigingen en kwetsbaarheden in het cyberdomein. Volgens het Cybersecurity Beeld Nederland (CSBN) gaat de grootste dreiging uit van staten en criminelen. Staten vormen vooral een dreiging in de vorm van diefstal van vertrouwelijke of concurrentiegevoelige informatie (cyberspionage). Criminelen richten zich met name op digitale fraude en diefstal van informatie. Door de toegenomen complexiteit, afhankelijkheid en kwetsbaarheid van ICT-gebaseerde producten en diensten is onze digitale weerbaarheid tegen deze en andere cyberdreigingen nog onvoldoende.

Naast deze dreigingen hebben we ook te maken met andersoortige uitdagingen in het cyberdomein. Zo zijn grote internationale private spelers een belangrijke factor geworden bij het bepalen van de spelregels in het cyberdomein en is er een grotere verwevenheid van de civiele en militaire domeinen. Daarnaast is de internationale beleidscontext van cybersecurity verbreed. Cybersecurity is niet in isolement tot stand te brengen en zal in samenhang moeten worden bezien met internetvrijheid (bijvoorbeeld vrijheid van meningsuiting en privacy) en maatschappelijke groei (zowel de economische als sociale voordelen die digitalisering biedt).

Deze ontwikkelingen maken een volgende stap in de aanpak van cybersecurity nodig. Dit op basis van de volgende visie:

> *Nederland zet samen met zijn internationale partners in op een veilig en open cyberdomein, waarin de kansen die digitalisering onze samenleving biedt volop worden benut, dreigingen het hoofd worden geboden en fundamentele rechten en waarden worden beschermd.*

In de tabel op de volgende pagina wordt in hoofdlijnen de stap weergegeven die met de NCSS2 wordt gemaakt.

De in de NCSS2 voorgestelde samenhang tussen veiligheid, vrijheid en maatschappelijke groei is een dynamische balans die tot stand moet komen in een constante open en pragmatische dialoog tussen alle stakeholders, zowel nationaal als internationaal. Benodigd is een helder governancemodel. Het uitgangspunt is daarbij dat verantwoordelijkheden zoals die in het fysieke domein gelden ook in het digitale domein genomen moeten worden. Om de dialoog tussen verschillende stakeholders te laten leiden naar een nieuw volwassenheidsniveau

1 Het cyberdomein is het conglomeraat van ICT-middelen en -diensten en bevat alle entiteiten die digitaal verbonden (kunnen) zijn. Het domein omvat zowel permanente als tijdelijke of plaatselijke verbindingen, evenals de gegevens (o.a. data, programmacode, informatie) die zich in dit domein bevinden, waarbij geen geografische beperkingen zijn gesteld.

NCSS1	NCSS2
Publiek-Privaat partnership	Privaat-Publieke participatie
Focus op structuren	Focus op netwerken / strategische coalities
Benoemen multi-stakeholdermodel	Verduidelijken onderlinge verhoudingen stakeholders
Capaciteitsopbouw nationaal gericht	Capaciteitsopbouw zowel nationaal als internationaal gericht
Generieke benadering: breed inzetten op weerstandverhogende maatregelen	Risicogebaseerde benadering: balans tussen bescherming belangen, dreiging belangen en geaccepteerd risico voor de samenleving
Uitgangspunten benoemen	(Beleids)visie weergeven
Van onbewust naar bewust	Van bewust naar bekwaam[2]

van cybersecurity zijn in het bijzonder de volgende drie sturingsdimensies van belang: (zelf)regulering, transparantie en kennisontwikkeling. Deze concepten zijn in verschillende vormen verweven in deze strategie.

De overheid zal een nadrukkelijker rol gaan spelen in het cyberdomein. Enerzijds door zelf te investeren in de veiligheid van de eigen netwerken en diensten. Anderzijds door partijen bij elkaar te brengen en beschermend op te treden als de veiligheid van bedrijven en burgers of de privacy van die laatste wordt bedreigd. Waar nodig zal de overheid kader- en normstellend optreden, bijvoorbeeld waar het gaat om veiligheidsvereisten aan vitale diensten en processen.

Van burgers wordt een zekere mate van cyberhygiëne (het toepassen van basis-veiligheidsvereisten) en eigen verantwoordelijkheid verwacht. De overheid faciliteert dit samen met het bedrijfsleven door het verbeteren van de digitale vaardigheden en het benadrukken van de zorgplicht van bedrijven en overheden richting hun klanten. Ook ICT-producten en -diensten moeten veilig zijn. Bedrijven en overheden moeten aanspreekbaar zijn op hun verantwoordelijkheid. Ook moeten zij transparant zijn over wat ze in het kader van cybersecurity aan maatregelen nemen en hoe ze omgaan met de gegevens van gebruikers. Het kabinet stelt zich ten doel dat burgers en bedrijven in 2017 hun zaken met de overheid digitaal en veilig kunnen afhandelen.

De geschetste integrale benadering (met betrokkenheid van alle partijen) gericht op de samenhang tussen veiligheid, vrijheid en maatschappelijke groei zal Nederland ook internationaal uitdragen.

Nederland wil een vooraanstaande rol spelen bij het zoeken naar nieuwe coalities voor defence, diplomacy en development waarin alle betrokken partijen vertegenwoordigd. Dit om te komen tot internationaal geaccepteerde normen en standaarden voor het handelen in het cyberdomein. Nederland zet daarom actief in op internationale samenwerking en neemt een duidelijk profiel in als bemiddelaar en knooppunt voor cybersecurity.

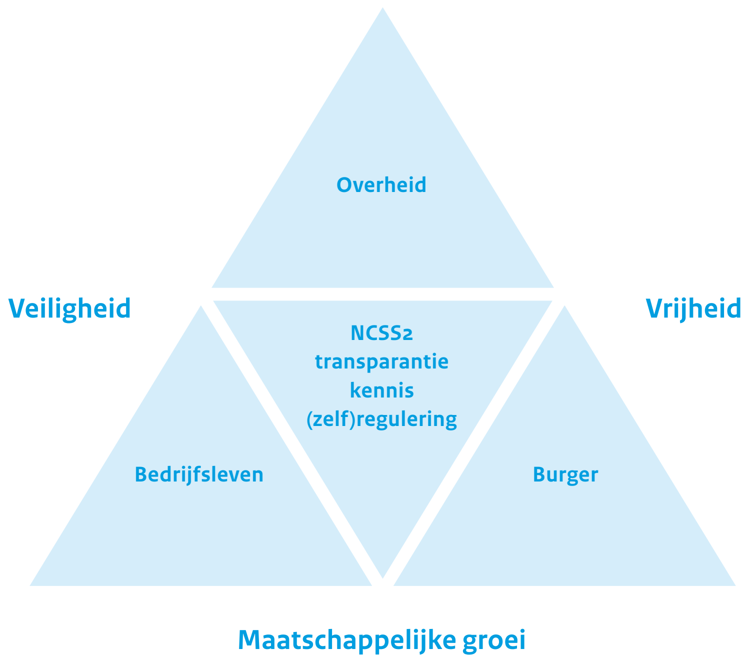
Op basis van de visie zet het kabinet in op de realisatie van de volgende ambities:

Nederland is leidend op het terrein van cybersecurity:

- *De Nederlandse samenleving weet op een veilige manier optimaal gebruik te maken van de voordelen van digitalisering.*
- *Het Nederlandse bedrijfsleven en de wetenschap lopen voorop op het gebied van security- en privacy-by-design.*
- *Samen met zijn internationale partners vormt Nederland een vooruitstrevende coalitie voor het beschermen van fundamentele rechten en waarden in het digitale domein.*

De realisatie van deze ambities wordt vormgegeven aan de hand van onderstaande strategische doelstellingen die

2 Niet alle partijen in de Nederlandse samenleving zijn zich voldoende bewust van cybersecurity. Aandacht hiervoor blijft nodig.



de leidraad vormen voor het actieprogramma 2014-2016. Over de voortgang zal jaarlijks worden gerapporteerd en indien nodig wordt het actieprogramma geactualiseerd.

1. Nederland is weerbaar tegen cyberaanvallen en beschermt zijn vitale belangen in het cyberdomein.
2. Nederland pakt cybercriminaliteit aan.
3. Nederland investeert in veilige en privacy-beschermende ICT-producten en -diensten.
4. Nederland bouwt coalities voor vrijheid, veiligheid en vrede in het cyberdomein.
5. Nederland beschikt over voldoende cybersecurity-kennis en -kunde en investeert in ICT-innovatie om onze cybersecuritydoelstellingen te behalen.

Binnen deze doelstellingen staan de volgende speerpunten centraal:

1 Aanpak vitaal: risicoanalyses, veiligheidseisen en informatiedeling

In het kader van de aanpak voor de bescherming van de vitale infrastructuur brengt de overheid samen met vitale partijen in beeld welke ICT-afhankelijke systemen, diensten en processen vitaal zijn. Hieraan is een programma gekoppeld dat op basis van risicoanalyses (basis)vereisten stelt aan de veiligheid hiervan.

2 Versterkte aanpak cyberspionage

De Nederlandse overheid zet zich in om het bewustzijn bij burgers, bedrijven, organisaties en overheden omtrent informatiebeveiliging en privacy te versterken. Ook zet de overheid in op prioriteit en capaciteit bij de inlichtingen- en veiligheidsdiensten om cyberdreigingen beter in kaart te brengen en geavanceerde aanvallen beter te onderzoeken en tegen te gaan. Hiervoor bundelen de inlichtingen- en veiligheidsdiensten hun cybercapaciteiten in een gezamenlijke Joint Sigint Cyber Unit (JSCU).

3 Haalbaarheidsonderzoek gescheiden netwerk vitaal

Er wordt een verkenning uitgevoerd in hoeverre het realiseren van een gescheiden ICT-netwerk voor (publieke en private) vitale processen op technisch en organisatorisch vlak mogelijk en wenselijk is. Met een gescheiden netwerk nemen de mogelijkheden om de continuïteit van vitale processen te borgen toe. Ook kunnen binnen het gescheiden netwerk eigen dataopslag of een cloud worden ontwikkeld. Hierdoor kan de privacy/integriteit van de data in deze opslag of cloud worden verbeterd.

4 Versterking civiel-militaire samenwerking

In het cyberdomein is sprake van een toegenomen verwevenheid van de civiele en militaire domeinen. Daarom zullen de mogelijkheden worden uitgewerkt om digitale capaciteiten van Defensie nationaal in te zetten bij het voorkomen en afweren van aanvallen op de civiele infrastructuur. Kernvraag daarbij is hoe kennis en

expertise optimaal gedeeld kunnen worden tussen civiele partijen en Defensie.

5 Versterking Nationaal Cyber Security Centrum

De positie van het NCSC wordt verstevigd door een versterkte structuur te bieden voor vertrouwde informatiedeling en -analyse en door in te zetten op een rol als kennisautoriteit. Het NCSC geeft vanuit deze expertrol gevraagd en ongevraagd advies aan aangesloten private en publieke partijen. Tenslotte verbreedt het NCSC zich op basis van de eigen detectiecapaciteit en de triagerol bij crises ook naar een Nationaal Cyber Security Operations Center (CSOC)[3], naast zijn rol van Computer Emergency Respons Team (CERT).

6 Internationale aanpak cybercriminaliteit: actualisatie en versterking (straf)wetgeving

Effectieve, snelle en efficiënte opsporing van cybercriminaliteit conform duidelijke regels is hard nodig. Schaarse capaciteit moet geconcentreerd worden ingezet bij kwetsbare sectoren en groepen. Nederland neemt een voortrekkersrol op zich bij het in internationaal verband komen tot grotere harmonisering van de wetgeving op het gebied van opsporing. Bijvoorbeeld binnen de Raad van Europa. Nederland zet tevens in op het versterken en uitbouwen van internationale samenwerkingsverbanden zoals het European Cybercrime Centre van Europol.

7 Gedragen standaarden en security en privacy by design

De overheid zet samen met private partners in op het ontwikkelen van standaarden die gebruikt worden om de veiligheid van ICT-producten en -diensten te verbeteren en privacy te beschermen.

8 Cyberdiplomatie: kennisknooppunt voor conflictpreventie

Nederland zet in op de ontwikkeling van een kennisknooppunt op het gebied van internationaal recht en cybersecurity. Doel van het kennisknooppunt is het bevorderen van het vreedzaam gebruik van het cyberdomein. Hiertoe zal Nederland kennis vanuit bestaande centra verbinden. Binnen het knooppunt worden internationale experts en beleidsmakers, diplomaten, militairen en NGO's samengebracht.

9 Taskforce cybersecurity onderwijs

Om de pool van cybersecurityexperts te vergroten en de cybersecurityvaardigheden van gebruikers te versterken, slaan bedrijfsleven en overheid de handen ineen voor een beter aanbod van ICT-onderwijs binnen zowel het lager, hoger als professioneel onderwijs. Er wordt een PPS taskforce Cybersecurity Onderwijs ingesteld, die zich richt op advisering over het aanbod van cybersecurity-onderwijs.

10 Stimuleren van innovatie in cybersecurity

Meer coördinatie op vraag en aanbod van innovatie is gewenst. Dit wordt bereikt door bestaande innovatie-initiatieven en het topsectorenbeleid aan elkaar te verbinden. Daarnaast zullen overheid, bedrijfsleven en wetenschap een cybersecurityplatform lanceren. Daar kunnen gevestigde bedrijven, studenten en onderzoekers elkaar vinden, inspireren en onderzoeksvraag en -aanbod op elkaar afstemmen. Ook het verder in PPS-verband uitvoeren van de (tweede editie van de) Nationale Cyber Security Research Agenda (NCSRA) draagt hieraan bij.

3 CSOC omvat naast respons meer aspecten van de cybersecurity-veiligheidsketen zoals awareness, weerbaarheid, detecteren, alerteren, rapporteren en crisisbeheersing.

We maken de beweging van bewust naar bekwaam. Kennisontwikkeling, transparantie en (zelf)regulering zijn daarbij van groot belang.

Steeds meer producten en diensten worden met het internet en elkaar verbonden. De vraag is hoe veilig dit is en wat dat voor onze privacy betekent.



1 Het belang van cybersecurity

1.1 INLEIDING

Het cyberdomein[4] is steeds meer verweven met ons dagelijks leven. Burgers, overheden en bedrijven gebruiken digitale toepassingen voor online interactie en transacties, efficiënter (samen)werken, communicatie en vermaak. Ook wordt apparatuur met ingebouwde ICT vaker verbonden met het internet: computers en telefoons, maar ook auto's, thermostaten en medische applicaties. Deze verregaande digitalisering dient niet alleen gemak, efficiëntie en plezier, maar is ook een belangrijke drijfveer voor innovatie en economische groei.

Kengetallen Nederlands gebruik internet[5]

- In 2012 telde Nederland 12,3 miljoen internetgebruikers.
- Nederland heeft 's werelds meest competitieve internetmarkt en het op één na hoogste percentage computers per huishouden (94% van de huishoudens).
- Nederlanders lopen voorop in het gebruik van innovatieve digitale diensten: 95% procent van de Nederlandse jongeren gebruikt sociale media; Nederland is koploper op het gebruik van internetbankieren in Europa en in 2012 winkelden circa 10 miljoen Nederlanders online.
- De omzet van de Nederlandse ICT-sector in Nederland was 29,8 miljard euro in 2011 (5% van het BBP).
- De ICT-sector is de meest innovatieve sector van Nederland. Meer dan tweederde van de ICT-bedrijven had onderzoeks- of innovatieve activiteiten in de periode 2008–2010.
- Nederland functioneert als Digital Gateway to Europe. Nederland staat samen met Duitsland en het Verenigd Koninkrijk in voor 18% van het wereldwijde internetverkeer door de aanwezigheid van drie grote internetknooppunten (Amsterdam, Berlijn en Londen).

Dat er risico's zijn verbonden aan gebruik van ICT is in de afgelopen jaren steeds duidelijker geworden door een aantal in het oog springende incidenten[6]. Ontwikkelingen als clouddiensten, mobiele diensten en innovatieve, op ICT-gebaseerde toepassingen introduceren vrijwel altijd nieuwe kwetsbaarheden.

> ***Cybersecurity** is het streven naar het voorkomen van schade door verstoring, uitval of misbruik van ICT en, indien er toch schade is ontstaan, het herstellen hiervan.*
>
> *De schade kan bestaan uit: aantasting van de betrouwbaarheid van ICT, beperking van de beschikbaarheid en schending van de vertrouwelijkheid en/of de integriteit van in ICT opgeslagen informatie.*

De digitale weerbaarheid van Nederland kan niet door de overheid alleen tot stand worden gebracht. Dit omdat de ICT-infrastructuur en de kennis van deze infrastructuur grotendeels in handen is van (internationale) private partijen. Cybersecurity is daarom de optelsom van de gezamenlijke inspanningen van overheden, bedrijfsleven, organisaties en burgers, zowel nationaal als internationaal. Daarbij is net als in de fysieke wereld ook in het digitale domein honderd procent veiligheid niet haalbaar.

4 Het cyberdomein is het conglomeraat van ICT-middelen en -diensten en bevat alle entiteiten die digitaal verbonden (kunnen) zijn. Het domein omvat zowel permanente als tijdelijke of plaatselijke verbindingen, evenals de gegevens (o.a. data, programmacode, informatie) die zich in dit domein bevinden, waarbij geen geografische beperkingen zijn gesteld.

5 ICT Kennis en Economie 2012, CBS.

6 Bijvoorbeeld: de DigiNotar-affaire, een gehackt gemeentelijk afvalwatersysteem en het Pobelka-botnet.

Relatie NCSS2 met strategische beleidsdocumenten:
De NCSS2 bouwt voort op de inzichten en aanbevelingen die voortkomen uit de volgende strategische beleidsdocumenten:

- De strategie Nationale Veiligheid (strategie NV) is erop gericht om aantasting van de vitale nationale belangen, die mogelijk kunnen leiden tot maatschappelijke ontwrichting, zoveel mogelijk te voorkomen[7]. Zowel in 2010 (cyberconflict) als in 2012 (cyberspionage) zijn scenario's omtrent digitale veiligheid meegenomen in de strategie Nationale Veiligheid.

- De Internationale Veiligheidsstrategie[8] richt zich op datgene wat Nederland ín en mét het buitenland onderneemt om zijn belangen veilig te stellen. Cybersecurity wordt in deze strategie als belangrijk thema genoemd, dat bij uitstek samen met onze Europese en internationale partners moet worden opgepakt.

- De Defensie Cyber strategie[9] richt zich op de rol die de krijgsmacht speelt in het digitale domein. Daarbij speelt dat militaire en civiele, publieke en private en nationale en internationale actoren in het digitale domein steeds meer met elkaar verweven zijn.

- In de Digitale Agenda[10] focust het kabinet op de bijdrage die ICT kan leveren aan de economische groei in Nederland. De Digitale Agenda zet de ambities neer wat betreft inzet van ICT voor groei en welvaart, inclusief de hiervoor benodigde randvoorwaarden: een open en snelle infrastructuur die met vertrouwen gebruikt kan worden en voldoende (benutting van) ICT-kennis.

- De bewustwordingsstrategie[11] informatieveiligheid voor overheidsbestuurders en -managers. Met de Taskforce Bestuur en informatieveiligheid dienstverlening voert het kabinet een actief bewustwordingsbeleid om de informatieveiligheid binnen de overheid op het gewenste niveau te brengen. Dit als belangrijke randvoorwaarde bij de uitwerking van de plannen van het kabinet rond de digitale overheid 2017. Maar ook met het oog op het Nationaal Uitvoeringsprogramma Dienstverlening en E-overheid (i-NUP) waarin een basisinfrastructuur wordt voltooid.

- In de brief e-privacy[12] worden randvoorwaarden beschreven die nodig zijn voor een goede bescherming van persoonsgegevens en de persoonlijke levenssfeer in de relatie tussen burgers en bedrijven in het bijzonder.

- De in 2013 verschenen Europese Cybersecurity strategie[13] is een belangrijke stap op weg naar een veilige digitale omgeving binnen Europa. De Nederlandse NCSS2 is in lijn met de uitgangspunten in de Europese Cybersecurity strategie en zet op basis daarvan nieuwe stappen.

- In het najaar van 2013 wordt een middellangetermijnvisie op de telecommarkt gepresenteerd aan de Tweede Kamer. Uitgangspunt van de visie is dat de telecommarkt niet los kan worden gezien van de ontwikkelingen op het internet en dat publieke waarden - zoals betrouwbaarheid en openheid - op de telecommarkt opnieuw moeten worden beoordeeld in het licht van de bredere context van de internet-economie.

7 De vijf vitale belangen zijn: territoriale veiligheid, fysieke veiligheid, economische veiligheid, ecologische veiligheid en sociale en politieke stabiliteit.

8 Internationale Veiligheidsstrategie, 21 juni 2013

9 Defensie Cyber Strategie TK 2011-2012 33 321, nr. 1

10 Kamerbrief 'Digitale Agenda.nl', TK 2010 – 2011, 29 515, nr. 331

11 Visiebrief digitale overheid 2017, TK 2012 – 2013, 26 643, nr. 280

12 Kabinetsvisie e-privacy: op weg naar gerechtvaardigd vertrouwen, 24 mei 2013

13 Cyber Security Strategie van de Europese Unie 'bescherming van open en vrij internet en kansen in digitale wereld (feb 2013) en bijbehorende conceptrichtlijn: Proposal for a Directive of the European Parliament and of the Council concerning measures to ensure a high common level of network and information security across the Union, februari 2013

1.2 DREIGINGEN

In juli 2013 is het derde Cybersecuritybeeld Nederland (CSBN) verschenen. De bevindingen uit dit CSBN[14] vormen een belangrijke bron voor een op risico[15] gebaseerde aanpak van cybersecurity. Uit het CSBN komt naar voren dat de grootste dreiging uitgaat van staten en criminelen.

Staten vormen vooral een dreiging in de vorm van diefstal van vertrouwelijke of concurrentiegevoelige informatie (cyberspionage) bij bedrijven, overheden en burgers. Diverse staten hebben de afgelopen jaren veel geïnvesteerd in cybercapaciteiten en beschikken daardoor over zeer geavanceerde mogelijkheden. Het is aannemelijk dat cyberspionage-activiteiten van deze landen wijdverbreid zijn en dat veel van deze activiteiten (nog) niet worden waargenomen.

Van criminelen blijft een grote dreiging uitgaan. Digitale fraude en diefstal van informatie zijn het meest voorkomend. Burgers, maar ook bedrijven en overheden zijn daarnaast regelmatig het slachtoffer van botnets en ransomware. Daarbij is een criminele cyberdienstensector, waarin hulpmiddelen via "cybercriminaliteit-as-a-service" commercieel beschikbaar worden gesteld, nadrukkelijk zichtbaar geworden. De toegang tot deze hulpmiddelen is goedkoper en laagdrempeliger geworden voor criminelen.

Ondanks dat er (onder andere op grond van de NCSS) goede initiatieven zijn gestart en maatregelen zijn genomen ter verhoging van de weerbaarheid en bewustwording, neemt de kwetsbaarheid van de samenleving nog toe. Bij veel organisaties is de digitale weerbaarheid nog onvoldoende. Relatief simpele maar belangrijke (technische) basismaatregelen (bijvoorbeeld het tijdig updaten van systemen of het wachtwoordenbeleid) zijn vaak nog niet doorgevoerd. Ook worstelen organisaties met legacysystemen. Het vervangen van deze verouderde systemen, waarvan vaak een wezenlijk deel van de informatievoorziening van organisaties afhankelijk is, is een complex en kostbaar probleem.

1.3 UITDAGINGEN

De toekomst laat zich slecht voorspellen op het dynamische terrein van cybersecurity. Wel is er een aantal uitdagingen te schetsen dat nu, maar ook op de lange termijn invloed heeft op de veiligheid en openheid van het cyberdomein:

- *Het internet der dingen (alles is verbonden aan het internet) en hyperconnectiviteit (alles wordt met elkaar verbonden)* bevorderen innovatie en brengen veel gebruikersgemak met zich mee. Tegelijkertijd roept het de vraag op of digitaal gekoppelde producten en diensten ook veilig zijn en welke implicaties dit heeft voor de privacy.
- *De hoeveelheid in digitale vorm beschikbare data neemt alleen maar toe;* de interesse in het verkrijgen van die data ook. Het werken met grote databestanden bij overheid en bedrijven, die in toenemende mate in de cloud worden opgeslagen, brengt risico's met zich mee.
- *Het speelveld in het cyberdomein wordt niet alleen bepaald door staten, maar ook door grote private partijen.* Governance in het cyberdomein is hierdoor complex en kan niet altijd in traditionele fora worden opgelost en vereist een multi-stakeholder benadering. Dat geldt voor veiligheidsstandaarden, maar evengoed voor het beschermen van fundamentele rechten en waarden.
- *In het cyberdomein is sprake van een toegenomen verwevenheid van de civiele en militaire domeinen door de grote wederzijdse afhankelijkheid van vergelijkbare ICT-systemen en -toepassingen en het complexe attributievraagstuk.* Bij militaire inzet van Nederland in het buitenland moet rekening worden gehouden met digitale aanvallen op civiele doelen in Nederland. Daarnaast kan er een beroep op cybercapaciteiten van Defensie worden gedaan bij de bescherming van de vitale nationale civiele infrastructuur in geval van grootschalige aanvallen. Heldere kaders over versterkte samenwerking in het cyberdomein zijn nodig.
- *De toegenomen complexiteit en afhankelijkheid van ICT-gebaseerde producten en diensten vergt een hoger kennisniveau.* Het gaat daarbij zowel om het kennisniveau van de gemiddelde gebruiker als om voldoende gekwalificeerde experts. Naar verwachting heeft Nederland in 2017 een tekort van 6800 ICT'ers.[16]

14 Het CSBN wordt elk jaar door het NCSC gepubliceerd en komt tot stand in nauwe samenwerking met publieke en private partijen.

15 Het risico wordt bepaald aan de hand van drie samenhangende factoren: belangen, dreigingen en weerbaarheid.

16 Gebaseerd op schattingen van Nederland ICT

We kunnen cybersecurity niet in isolement tot stand brengen, het zal in relatie gebracht moeten worden met onderwerpen als fundamentele rechten en waarden en maatschappelijke groei.



2 Visie

Nederland zet samen met zijn internationale partners in op een veilig en open cyberdomein, waarin de kansen die digitalisering onze samenleving biedt volop worden benut, dreigingen het hoofd worden geboden en fundamentele rechten en waarden worden beschermd.

2.1 INLEIDING: NAAR EEN NIEUWE BENADERING EN WERKWIJZE

In 2011 verscheen de eerste Nationale Cybersecurity Strategie (NCSS1). Sinds die tijd is er veel gebeurd. De samenwerkende partijen binnen het Nationaal Cyber Security Centrum zijn erin geslaagd een beter inzicht in de dreiging te geven. Het derde Cybersecuritybeeld Nederland maakt daarmee een gerichtere aanpak mogelijk. Daarnaast wordt de internationale inzet steeds belangrijker. Afspraken over samenwerking, (gedrags) normen en standaarden moeten in Europees en in breder internationaal verband worden gemaakt. De internationale beleidscontext is bovendien verbreed. Cybersecurity is niet in isolement tot stand te brengen en zal in relatie gebracht moeten worden met onderwerpen als fundamentele rechten en waarden en maatschappelijke groei. Deze ontwikkelingen maken een volgende stap in de aanpak van cybersecurity nodig.

In de tabel onderaan wordt in hoofdlijnen de stap weergegeven die met de NCSS2 wordt gemaakt.

2.2 VEILIGHEID, VRIJHEID EN MAATSCHAPPELIJKE GROEI

De maatregelen in het kader van cybersecurity vergen maatwerk. Dat wordt op drie manieren vormgegeven. Ten eerste door maatregelen toe te snijden op het probleem dat ze moeten oplossen (risk-based), ten tweede door cybersecurity steeds in samenhang te bezien met maatschappelijke groei (zowel de economische als sociale voordelen die digitalisering biedt) en ten derde door het waarborgen van fundamentele rechten en waarden. Deze samenhang tussen veiligheid, vrijheid en maatschappelijke groei is een dynamische balans die tot stand moet

NCSS1	NCSS2
Publiek-Privaat Partnership	Privaat-Publieke Participatie
Focus op structuren	Focus op netwerken / strategische coalities
Benoemen multi-stakeholdermodel	Verduidelijken onderlinge verhoudingen stakeholders
Capaciteitsopbouw nationaal gericht	Capaciteitsopbouw zowel nationaal als internationaal gericht
Generieke benadering: breed inzetten op weerstand verhogende maatregelen	Risicogebaseerde benadering: balans tussen bescherming belangen, dreiging belangen en geaccepteerd risico voor de samenleving
Uitgangspunten benoemen	(Beleids)visie weergeven
Van onbewust naar bewust	Van bewust naar bekwaam[17]

17 Niet alle partijen in de Nederlandse samenleving zijn zich voldoende bewust van cybersecurity. Aandacht hiervoor blijft nodig.



komen in een constante open en pragmatische dialoog tussen alle stakeholders, zowel nationaal als internationaal.

2.2.1. VEILIGHEID

Cybersecurity gaat zowel om de veiligheid van ICT als om de veiligheid van daarin opgeslagen informatie. Uitval van op ICT-gebaseerde diensten en processen kan grote maatschappelijke gevolgen hebben. Bij uitval van vitale diensten en processen is er zelfs kans op maatschappelijke ontwrichting. Het beschermen van persoonsgegevens, staatsgeheimen en andere gevoelige informatie is essentieel voor het vertrouwen dat partijen hebben in het cyberdomein.

Het verwerken van persoonsgegevens en de bescherming van de persoonlijke levenssfeer is mede op basis van Europese wetgeving in Nederland aan strikte normen en toezicht gebonden. Recente onthullingen over heimelijke activiteiten van staten gericht op het verwerven van informatie onderstrepen het belang van bewustzijn over informatiebeveiliging bij alle stakeholders, evenals de noodzaak tot het verhogen van de weerbaarheid van onze vitale infrastructuur tegen dergelijke activiteiten.

Om het gewenste niveau van veiligheid te bereiken is een brede aanpak nodig door de gehele veiligheidsketen voor ICT[18]. Dat begint bij inzicht in de dreiging en een sterke preventieve aanpak, maar vereist tevens een effectieve responsstrategie. Dit betekent dat ook de criminaliteit in het cyberdomein succesvol moet worden aangepakt. Dit vraagt om verduidelijking van de handhavende rol van de politie en actualisering van de mogelijkheden en bevoegdheden om opsporing en vervolging in het cyberdomein effectief te laten zijn.

2.2.2 VRIJHEID

Het beschermen van fundamentele rechten en waarden vergt inzet van vele partijen en dient in (inter)nationaal verband te gebeuren. De aanpak die wordt voorgestaan is het ontwikkelen van internationale normen en standaarden. Naast overheden is hier een belangrijke rol weggelegd voor partijen uit de private sector en maatschappelijke organisaties. Nederland maakt zich hier onder meer hard voor in kader van de Verenigde Naties, tijdens internationale cyberspace conferenties zoals gehouden in Londen, Budapest en Seoul, in andere multi-stakeholdersettings zoals het Internet Governance Forum, door het bevorderen van de principes van cybersecurity die zijn uitgebracht door het World Economic Forum en bij de ontwikkeling van vertrouwenwekkende maatregelen tussen staten, zoals door de Organisatie voor Veiligheid en Samenwerking in Europa (OVSE).

Een goed voorbeeld van de multi-stakeholderbenadering is de door Nederland geïnitieerde *Freedom Online Coalition*, waarbij zich inmiddels 21 landen hebben aangesloten die gezamenlijk een krachtige lobby vormen. Nederland heeft de ambitie om deze coalitie verder te laten groeien. Nu moeten we een stap verder gaan door de ontwikkelde

18 De veiligheidsketen omvat: pro-actie, preventie, preparatie, repressie en nazorg (herstel).

uitgangspunten integraal onderdeel te laten zijn van overleggen over cybersecuritynormen en -standaarden en deze mee te nemen in het ontwerp van nieuwe innovatieve producten en diensten.

2.2.3 MAATSCHAPPELIJKE GROEI

De innoverende kracht die uitgaat van verdergaande digitalisering is een belangrijke stimulans voor maatschappelijke groei. Het gaat daarbij zowel om economische groei als om de mogelijkheden die digitalisering biedt aan de samenleving, bijvoorbeeld in de vorm van onderwijstoepassingen, mogelijkheden tot het onderhouden van sociale contacten, maar ook verbeterde overheidsvoorzieningen. Door de kabinetsdoelstelling om het mogelijk te maken dat burgers en bedrijven in 2017 hun zaken met de overheid digitaal kunnen afhandelen, wordt een extra slag in de realisatie van de iOverheid gemaakt.[19] Daarmee wordt het maatschappelijk belang van de iOverheid nog groter. Maatregelen op het gebied van veiligheid en cybersecurity zijn daarom essentieel en brengen de nodige investeringen met zich mee.

Organisaties beseffen in toenemende mate dat door te investeren in cybersecurity grote kosten en reputatieschade kunnen worden vermeden. Deze strategie wil bevorderen dat meer Nederlandse bedrijven cybersecurity ook als concurrentievoordeel gaan ervaren.

Het toenemende belang dat door de kritische consument gehecht wordt aan veiligheid en privacy is een kans voor Nederlandse bedrijven om te investeren in innovatieve producten en diensten die hier in het ontwerp rekening mee houden. De overheid zal hierbij een stimulerende rol vervullen door in haar inkoopvoorwaarden cybersecurityvereisten op te nemen.

2.3 HELDERE ROLLEN, ACTIEVE PARTICIPANTEN

Het cyberdomein omvat een veelheid aan partijen en actoren die in toenemende mate met elkaar verbonden en van elkaar afhankelijk zijn. Om veilig te handelen in het cyberdomein, waar een grote (keten)afhankelijkheid bestaat tussen partijen, betekent dit dat burgers, bedrijven, organisaties en overheden actief participeren (doe-democratie[20]) op grond van een heldere rolverdeling en een grote mate van transparantie. Het uitgangspunt is dat verantwoordelijkheden die in het fysieke domein gelden, ook in het digitale domein genomen moeten worden. Hoe die rollen zich precies ten opzichte van elkaar verhouden, zal in de toekomst blijken. De richting waarin de actoren zich bewegen wordt hier nader toegelicht.

2.3.1 DE INTERVENIËRENDE OVERHEID: FACILITEREN, BESCHERMEN EN STUREN

Veiligheid is een kerntaak van de overheid, ook in het cyberdomein. Het tegengaan van cybercriminaliteit en cyberspionage en het voorkomen van maatschappelijke ontwrichting door cyberincidenten zijn dan ook belangrijke prioriteiten voor de overheid. Uitgangspunten zijn daarbij een risk-based benadering, versterkte samenwerking en zelf het goede voorbeeld geven door te investeren in de veiligheid van de eigen netwerken en diensten.

Daarnaast heeft de overheid een verantwoordelijkheid ten aanzien van de online veiligheid en privacy van burgers. De bescherming van waardevolle en persoonlijke informatie van burgers en bedrijven en het aanpakken van cybercriminaliteit blijven daarom speerpunten. In mei 2013 is de kabinetsvisie op e-privacy verschenen. Doel is ervoor te zorgen dat burgers een betere controle krijgen over wat er gebeurt met hun persoonsgegevens door het opnemen van de eis van toestemming. Organisaties dienen zorgvuldig, transparant en conform de wet om te gaan met informatie die de burger hen heeft verstrekt; burgers moeten organisaties daarop kunnen aanspreken. Ten slotte heeft de overheid een taak bij het stimuleren en faciliteren van initiatieven gericht op het verhogen van de cybersecurity.

De overheid treedt indien nodig sturend op. Daarbij kunnen regels, normen of standaarden worden vastgesteld, bijvoorbeeld voor de vitale infrastructuur. Samen met vitale partijen stelt de overheid cybersecurityvereisten op waar dat nog niet het geval is. Bestaande (sectorale) toezichthouders zullen vervolgens eveneens daar waar dat nog niet het geval is hun rol moeten verbreden om ook cybersecurity te omvatten, waarbij overlap/dubbeling dient te worden voorkomen.

Het NCSC geeft als kennisautoriteit gevraagd en ongevraagd advies wanneer majeure kwetsbaarheden worden geconstateerd of bij (dreigende) crisissituaties. Het is vervolgens aan de organisaties zelf deze adviezen op te volgen, dan wel transparant te zijn over de redenen waarom dit niet is gebeurd. Dit geldt zeker waar het overheidspartijen betreft, ook richting de eigen toezichthouder(s) en/of vakdepartementen.

19 Visiebrief digitale overheid 2017 23 mei 2013 kenmerk 2013-0000306907

20 Kabinetsstandpunt stimulering van een vitale samenleving, de Doe Democratie, Kamerstukken II, 2012-2013, 33400-VII nr. 79

2.3.2 DE BEKWAME BURGER: CYBERHYGIËNE EN EIGEN VERANTWOORDELIJKHEID

Van burgers mag een zekere basis-cyberhygiëne en bekwaamheid worden verwacht als zij ICT gebruiken, bijvoorbeeld bij het surfen op het web. Denk aan voorzichtig zijn met persoonlijke gegevens, het uitvoeren van updates, het gebruik van sterke wachtwoorden en het in evenwicht brengen van functionaliteit en cybersecurity. De overheid zet in op het vergroten van de digitale weerbaarheid van overheid, burgers en bedrijfsleven. Dit door bewustwordingscampagnes, het vergroten van de digitale vaardigheden, onderzoek en innovatie en het ondersteunen van maatschappelijke organisaties en initiatieven in het kader van doe-democratie. In dat kader past ook een beleid dat responsible disclosure ondersteunt en hindernissen hiervoor wegneemt. Hiermee wordt het mogelijk gemaakt dat bewuste en betrokken burgers overheden, bedrijven en instellingen op een veilige manier op de hoogte kunnen stellen van ontdekte kwetsbaarheden in hun (ICT-) beveiliging.

2.3.3 VERANTWOORDELIJKE BEDRIJVEN: ZORGPLICHT EN AANSPREEKBAAR OP VERANTWOORDELIJKHEID

Van burgers kan niet meer verwacht worden dat ze de steeds complexere ICT-diensten en producten, zoals aangeboden door grote internationale spelers, volledig kunnen doorgronden en beoordelen op veiligheids- en privacyaspecten. Hier ligt dan ook een duidelijke verantwoordelijkheid voor ICT-leveranciers en -producenten. Security en privacy by design zouden meer dan nu standaard ontwerpbeginselen moeten zijn.

Aanbieders van ICT-netwerken en -diensten of andere op ICT gebaseerde diensten hebben een specifieke verantwoordelijkheid (zorgplicht) richting hun klanten. Invulling van deze verantwoordelijkheid dient bij voorkeur door zelfregulering tot stand te komen. Een voorbeeld daarvan is de bestrijding van botnets, waarin Internet Service Providers (ISP)'s een cruciale rol spelen.

De afhankelijkheden in het digitale domein komen ook tot uitdrukking in de keten van producenten, leveranciers en afnemers. Deze onderlinge afhankelijkheden zullen door de ketenpartners moeten worden besproken. Dit om te komen tot gezamenlijke afspraken over minimumvereisten, interoperabiliteit en vertrouwde informatiedeling. Ook is het zo mogelijk de veiligheid van de gehele keten te versterken. Verzekeraars kunnen een belangrijke rol spelen bij het verzekeren van restrisico's.

2.3.4 (ZELF)REGULERING, TRANSPARANTIE EN KENNIS ALS STURINGSMECHANISMEN

Nederland werkt toe naar een actieve participatie van burgers, bedrijven en overheid in het digitale domein. Dit binnen een context van een steeds groter wordende onderlinge afhankelijkheid tussen deze actoren en een complexe omgeving waarin continu naar een balans moet worden gezocht tussen veiligheid, vrijheid en maatschappelijke groei.

Dit betekent dat er stappen moet worden gezet van onbewust naar bewust naar bekwaam. Om deze beweging naar een nieuw volwassenheidsniveau van cybersecurity mogelijk te maken, zijn in het bijzonder de volgende drie sturingsdimensies van belang: (zelf)regulering, transparantie en kennisontwikkeling. Deze concepten zijn in verschillende vormen verweven in deze strategie. (Zelf) regulering omvat het ontwikkelen van standaarden, maar ook een concept als zorgplicht. Transparantie is een randvoorwaarde voor het versterken van vertrouwen tussen de actoren. Een voorbeeld zijn heldere rapportages over de maatregelen die overheid en bedrijfsleven nemen ter bevordering van cybersecurity en rondom privacy. Kennisontwikkeling in de breedste zin (bewustwording, onderwijs, innovatie) is nodig om te zorgen dat alle actoren hun verantwoordelijkheid kunnen nemen en optimaal profiteren van de kansen die digitalisering biedt.

2.4 INTERNATIONALE VISIE EN INZET: EEN GEÏNTEGREERDE BENADERING

Nederland is als open economie gebaat bij een stabiel en vrij toegankelijk cyberdomein. Aangezien cybersecurity en internationale samenwerking onlosmakelijk met elkaar verbonden zijn, zal Nederland ook buiten de eigen grenzen de eigen integrale publiek-private cybersecurity-aanpak propageren. De ontwikkelde benadering waarin defence, diplomacy en development samenkomen bij internationale missies om de stabiliteit in het betreffende gebied te vergroten (crisisbeheersing en nation building), is de inspiratie voor de integrale Nederlandse inzet in het cyberdomein[21].

Nederland wil een vooraanstaande rol spelen bij het zoeken naar nieuwe coalities, waarin alle betrokken partijen vertegenwoordigd zijn om te komen tot internationaal geaccepteerde normen en standaarden voor het handelen in het cyberdomein. Daarom zet Nederland actief in op internationale samenwerking en neemt Nederland een duidelijke rol in als bemiddelaar en knooppunt voor cybersecurity.

21 Dit wordt ook wel de 3D-benadering genoemd.

2.4.1. DEFENCE

Defence (verdediging) omvat in het cyberdomein niet alleen de militaire capaciteiten, maar ook het brede civiele spectrum van de capaciteiten van inlichtingen- en veiligheidsdiensten, politie, nationale cybersecuritycentra en bedrijven met hun eigen responscapaciteiten. Dit is een complex geheel waarbinnen goede afspraken en coördinatie randvoorwaardelijk zijn, zowel nationaal als internationaal. Versterkte civiel-militaire samenwerking is dan ook nodig.

Om de inzetbaarheid van de Nederlandse krijgsmacht te waarborgen en haar effectiviteit te verhogen, versterkt Defensie haar digitale weerbaarheid en ontwikkelt zij het vermogen om, binnen de geldende wettelijke kaders, cyber operations uit te voeren. Het betreft hier zowel het vermogen om de eigen netwerken en systemen te beschermen tegen aanvallen als de capaciteit voor offensieve maatregelen. De digitale capaciteiten van Defensie kunnen nationaal worden ingezet op verzoek van civiele autoriteiten. Deze capaciteiten zullen ook bij internationale operaties worden ingezet, zowel als onderdeel van het eigen vermogen als voor het versterken of opbouwen van de capaciteiten van lokale autoriteiten. De capaciteiten van de krijgsmacht dragen zo bij aan de geïntegreerde benadering die Nederland voorstaat.

De NAVO kan een belangrijke rol spelen als facilitator. Te denken valt aan het bevorderen van nationale capaciteitsopbouw, verbeterde informatie-uitwisseling en interoperabiliteit en publiek-private samenwerking. Nederland zet daarnaast in op deelname aan oefeningen en versterkte samenwerking tussen EU en NAVO, waarbij overlap van capaciteiten moet worden vermeden.

Samenwerking in EU-verband zal zich in het kader van defence vooral richten op crisismanagement, pan-Europese oefeningen en effectieve opsporing en vervolging van cybercriminaliteit. In internationaal verband blijft Nederland het belang van bredere ratificering van het cybercriminaliteit verdrag van de Raad van Europa (Boedapest conventie) uitdragen. Goede samenwerking tussen nationale Computer Emergency Response Teams (CERTs) is van cruciaal belang om dreigingen, kwetsbaarheden en incidenten vroegtijdig te signaleren en om snel op te kunnen treden. In Nederland vervult het NCSC deze rol. Het verder uitbouwen en versterken van bestaande samenwerkingsverbanden zoals EGC en FIRST hebben voor Nederland prioriteit. Bij deze samenwerkingsverbanden staan flexibiliteit en onderling vertrouwen voorop.

2.4.2 DIPLOMACY

Nederland vindt het belangrijk te zoeken naar mechanismen die zorgen voor stabiliteit in het cyberdomein. Dat doen we door te investeren in formele en informele samenwerkingsverbanden, binnen en buiten de EU, globaal en in multi-stakeholdersettings. Daarom wil Nederland, met zijn positie op het terrein van internationaal recht, bijdragen aan de discussies over het toepassen van de rechtsregels in het cyberdomein. Aanvullend daaraan zullen instrumenten voor cyberdiplomatie geformuleerd moeten worden. Dit kan de vorm krijgen van zogeheten vertrouwenwekkende maatregelen, 'rules of the road', of gedragsnormen.[22] Met Den Haag als stad van internationale vrede en veiligheid wil Nederland zich ontwikkelen tot 'internationaal centrum van cyberdiplomacy' waar diplomaten, beleidsmakers en cyberexperts bij elkaar komen.

2.4.3 DEVELOPMENT

Dreigingen in het digitale domein zijn grenzeloos. Nederland is er dan ook zeer bij gebaat dat landen in staat zijn deze dreigingen het hoofd te bieden. Vanuit het NCSC zal ingezet worden op het versterken van CERT-capaciteiten in landen die daarom verzoeken.

Nederland ondersteunt de capaciteitsopbouw in de EU door onder andere de implementatie van de EU Cyber Security Strategie. Doel daarbij is om een basisniveau van veiligheid en een level playing field binnen Europa te creëren. Het verder brengen van de cybersecurity-aanpak in Europees kader zal een belangrijk punt zijn tijdens het Nederlandse EU-voorzitterschap in 2016. Thema's waar Nederland zich in Europees verband sterk voor wil maken zijn naast de genoemde versterkte CERT-samenwerking:

- Behouden van de open standaarden, content en interoperabiliteit van het internet
- Stimuleren van innovatie op veilige ICT-producten (security by design)
- Veiligheidseisen voor nieuwe en bestaande (embedded) ICT.

22 Startpunt voor Nederland zijn in dit verband het Handvest van de VN en de Geneefse en Haagse conventies.

Bekwame gebruikers en voldoende cybersecurity experts zijn noodzakelijk om optimaal gebruik te maken van de kansen die digitalisering ons biedt en weerbaar te zijn tegen de steeds geavanceerdere dreiging.



3 Aanpak

De Nederlandse visie op cybersecurity laat zich in dit hoofdstuk vertalen naar een concrete aanpak. In paragraaf 3.1 worden de Nederlandse cybersecurity-ambitie en de strategische doelstellingen die deze ondersteunen weergegeven. In paragrafen 3.2 tot en met 3.6 worden de NCSS2 doelstellingen toegelicht en worden per doelstelling de belangrijkste speerpunten weergegeven. In bijlage 1 is het actieprogramma opgenomen. Hierin staan de actiepunten die in het kader van de NCSS2 worden uitgevoerd.

3.1 AMBITIE EN STRATEGISCHE DOELSTELLINGEN

Op basis van de visie zet het kabinet in op de realisatie van de volgende ambities:

Nederland is leidend op het terrein van cybersecurity:

- *De Nederlandse samenleving weet op een veilige manier optimaal gebruik te maken van de voordelen van digitalisering.*
- *Het Nederlandse bedrijfsleven en de wetenschap lopen voorop op het gebied van security- en privacy-by-design.*
- *Samen met zijn internationale partners vormt Nederland een vooruitstrevende coalitie voor het beschermen van fundamentele rechten en waarden in het digitale domein.*

De realisatie van deze ambities wordt vormgegeven aan de hand van onderstaande strategische doelstellingen. Deze doelstellingen staan centraal in het actieprogramma 2014-2016. Over de voortgang van dit actieprogramma zal jaarlijks worden gerapporteerd en indien nodig wordt het actieprogramma geactualiseerd.

1. Nederland is weerbaar tegen cyberaanvallen en beschermt zijn vitale belangen in het cyberdomein.
2. Nederland pakt cybercriminaliteit aan.
3. Nederland investeert in veilige en privacybeschermende ICT-producten en -diensten.
4. Nederland bouwt coalities voor vrijheid, veiligheid en vrede in het cyberdomein.
5. Nederland beschikt over voldoende cybersecurity-kennis en -kunde en investeert in ICT-innovatie om onze cybersecurity doelstellingen te behalen.

3.2 NEDERLAND IS WEERBAAR TEGEN CYBERAANVALLEN EN BESCHERMT ZIJN VITALE BELANGEN IN HET CYBERDOMEIN

Onze vitale infrastructuur is in toenemende mate afhankelijk van ICT-systemen. Uitval of verstoring van deze systemen of het schenden van de vertrouwelijkheid van daarin opgeslagen informatie door staten en criminelen heeft grote impact. Het kan zelfs leiden tot maatschappelijke ontwrichting. Er is sprake van een toegenomen verwevenheid tussen militaire en civiele, publieke en private en nationale en internationale dimensies in het digitale domein. Zo kan de nationale veiligheid in gevaar worden gebracht door een grootschalige digitale aanval op één of meer private organisaties[23]. De snelheid waarmee dergelijke aanvallen zich kunnen manifesteren en ontwikkelen vraagt om een snelle, gecoördineerde en flexibele reactie en het vroegtijdig betrekken van de belangrijkste spelers.

Het is daarom van groot belang dat we meer zicht krijgen op de vitale processen en diensten en op het risico dat ze lopen. Van belang is daarbij ook kritisch te kijken naar de achterliggende ICT-ketenstructuur en 'legacy' systemen. Op basis van deze risicobenadering zullen we de weerbaarheid van vitale diensten en processen verhogen en inzetten op een effectieve gezamenlijke respons: publiek-privaat, civiel-militair en met behulp van onze internationale partners.

1 Aanpak vitaal: risicoanalyses, veiligheidseisen en informatiedeling

In het kader van de aanpak voor de bescherming van de vitale infrastructuur brengt de overheid samen met vitale partijen in beeld welke ICT-afhankelijke systemen, diensten en processen vitaal zijn. Hieraan is een programma gekoppeld dat op basis van risicoanalyses (basis) vereisten stelt aan de veiligheid ervan.

Tevens wordt een trainingsprogramma voor respons op grootschalige ICT-incidenten ingericht. In samenwerking met haar partners richt het Nationaal Cyber Security Centrum een nationaal detectie- en responsnetwerk in

23 Spraakmakende digitale aanvallen die grote schade teweeg hebben gebracht of potentieel ontwrichtend hadden kunnen zijn - zoals DigiNotar in Nederland, Stuxnet in Iran en de digitale aanval op Aramco in Saoedi-Arabië - waren allen niet gericht tegen militaire doelen maar tegen strategische civiele doelen.

voor de Rijksoverheid en overige vitale sectoren. Met deze netwerken wordt, omkleed met waarborgen op het gebied van onder meer vertrouwelijkheid en privacy, toegewerkt naar het real-time analyseren en delen van dreigingsinformatie.

2 Versterkte aanpak cyberspionage

De Nederlandse overheid zet zich in om het bewustzijn bij burgers, bedrijven, organisaties en overheden omtrent informatiebeveiliging en privacy te versterken. Dit houdt enerzijds in dat bewustwordingscampagnes zich mede gaan richten op het vergroten van kennis en inzicht op het risico van cyberspionage. Anderzijds zet de overheid in op prioriteit en capaciteit bij de inlichtingen- en veiligheidsdiensten om cyberdreigingen beter in kaart te brengen en geavanceerde aanvallen beter te onderzoeken en tegen te gaan. Hiervoor bundelen de inlichtingen- en veiligheidsdiensten hun cybercapaciteiten in een gezamenlijke Joint Sigint Cyber Unit (JSCU). Daarnaast zal de overheid prioriteit geven aan de betere bescherming van de gegevens die burgers met de overheid delen en hen meer transparantie over dit beheer geven.

3 Haalbaarheidsonderzoek gescheiden netwerk vitaal

Er wordt een verkenning uitgevoerd om te bezien in hoeverre het realiseren van een gescheiden ICT-netwerk voor (publieke en private) vitale processen op technisch en organisatorisch vlak mogelijk en wenselijk is. Met een gescheiden netwerk nemen de mogelijkheden om de continuïteit van vitale processen te borgen toe. Ook kunnen binnen het gescheiden netwerk eigen dataopslag of een cloud worden ontwikkeld. Hierdoor kan de privacy/integriteit van de data in deze opslag of cloud worden verbeterd.

4 Versterking civiel-militaire samenwerking

Digitale middelen maken in toenemende mate integraal deel uit van het militaire optreden. Om de inzetbaarheid van de Nederlandse krijgsmacht te waarborgen en haar effectiviteit te verhogen, versterkt Defensie haar digitale weerbaarheid en ontwikkelt zij het vermogen om cyber operations uit te voeren. In het cyberdomein is sprake van een toegenomen verwevenheid van de civiele en militaire domeinen. Daarom zullen de mogelijkheden worden uitgewerkt om digitale capaciteiten van Defensie nationaal in te zetten bij het voorkomen en afweren van aanvallen op de civiele infrastructuur. Kernvraag daarbij is hoe kennis en expertise optimaal gedeeld kunnen worden tussen civiele partijen en Defensie.

5 Versterking Nationaal Cyber Security Centrum

Het NCSC heeft zich in korte tijd ontwikkeld tot spil in het publiek-private cybersecurity-netwerk. Tegelijkertijd zijn mede door een aantal grote incidenten de verwachtingen ten aanzien van de rol van het NCSC gegroeid. Om hier invulling aan te geven, wordt de positie van het NCSC verstevigd door een versterkte structuur te bieden voor vertrouwelijke informatiedeling en -analyse en in te zetten op een rol als kennisautoriteit. Het NCSC geeft vanuit deze expertrol gevraagd en ongevraagd advies aan aangesloten private en publieke partijen. Tenslotte verbreedt het NCSC zich op basis van de eigen detectiecapaciteit en de triagerol bij crises ook naar een Nationaal Cyber Security Operations Center (CSOC)[24], naast zijn rol van Computer Emergency Respons Team (CERT).

3.3 NEDERLAND PAKT CYBERCRIME AAN

Cybercriminaliteit is een veel voorkomende en toenemende bedreiging voor alle burgers en organisaties in het cyberdomein. Om adequate bescherming tegen cybercriminaliteit te bieden, zal Nederland de bestrijding van cybercriminaliteit prioriteren door de huidige capaciteiten op het gebied van opsporing en vervolging te versterken. Geactualiseerde wetgeving, nauwe samenwerking en informatie-uitwisseling door de verschillende betrokken spelers is hierbij van belang. Nederland zal actief samenwerkingsverbanden op zowel nationaal als internationaal niveau (bijvoorbeeld in EU-kader) zoeken en verdiepen om een omvattende en doortastende aanpak van cybercriminaliteit te bewerkstelligen.

6 Internationale aanpak cybercriminaliteit: actualisatie en versterking (straf)wetgeving

Effectieve, snelle en efficiënte opsporing van cybercriminaliteit conform duidelijke regels is hard nodig. Schaarse capaciteit wordt geconcentreerd ingezet bij kwetsbare sectoren en groepen. Nederland zal een voortrekkersrol op zich nemen bij het internationaal komen tot grotere harmonisering van de wetgeving op het gebied van opsporing. Nederland zet tevens in op het versterken en uitbouwen van internationale samenwerkingsverbanden zoals het European Cyber Crime Centre EC3, bij Europol. Bij deze internationale samenwerking hoort ook het op termijn mogelijk vormgeven van arbitrage tussen landen wanneer deze niet tevreden zijn over de geboden assistentie bij het opsporingsproces. Nederland neemt actief deel aan internationaal overleg en gerelateerde activiteiten, zoals het comité van verdragsluitende partijen, het Raad van Europa cybercrimeverdrag, de “EU policy cycle

24 CSOC omvat naast respons meer aspecten van de cybersecurity-veiligheidsketen zoals awareness, weerbaarheid, detecteren, alerteren, rapporteren en crisisbeheersing.

on organised crime" en de discussie binnen UNODC over een VN-verdrag op het gebied van cybercrime. Daarnaast ligt in Nederland een wetstraject voor waarin voorstellen worden gedaan om politie en Openbaar Ministerie meer bevoegdheden te geven bij de opsporing in de digitale ruimte.

3.4 NEDERLAND INVESTEERT IN VEILIGE EN PRIVACY BESCHERMENDE ICT-PRODUCTEN EN -DIENSTEN

Steeds meer op ICT-gebaseerde producten en -diensten worden verbonden met publieke netwerken zoals het internet en zijn op hun beurt weer gekoppeld aan andere producten en diensten. Deze ontwikkeling biedt veel voordelen, maar brengt tegelijkertijd nieuwe veiligheidsrisico's met zich mee. In het fysieke domein is het heel gebruikelijk veiligheids- en kwaliteitseisen aan producten en diensten te stellen alvorens deze in de markt te zetten. In het digitale domein daarentegen is dat veel minder het geval. Zo worden de impact en neveneffecten van ICT-producten of diensten als online investeren of winkelen nauwelijks meegenomen in de keuze deze in gebruik te nemen. Veiligheids- en privacy-eisen helpen organisaties en burgers beter tegen veiligheidsrisico's te beschermen. De digitale dienstverlening van de overheid dient hierbij een voorbeeldfunctie te hebben.

Innovatie, veiligheid en privacy kunnen in de ontwerpfase van producten en diensten niet alleen uitstekend samengaan, maar helpen ook deze producten en diensten zich op positieve wijze te onderscheiden. De inspanningen van overheid en bedrijfsleven moeten er daarom op gericht zijn dat ook te laten lonen. Samenwerking met internationale partners is daarbij essentieel.

7 Gedragen standaarden en security en privacy by design

De overheid zet samen met private partners in op het ontwikkelen van standaarden die gebruikt worden om de veiligheid van ICT-producten en -diensten te verbeteren en privacy te beschermen. Hiertoe zal de overheid ook in internationaal verband de dialoog aangaan met relevante private partijen en waar nodig kader- en normstellend optreden ter bescherming van de privacy en veiligheid van gebruikers. Waar mogelijk gebeurt dit in Europees of breder internationaal verband en wordt aangesloten bij bestaande (internationale) standaarden en good practices[25]. Door standaarden op te nemen in aanbestedingseisen stimuleert de overheid de implementatie ervan als 'launching customer'.

3.5 NEDERLAND BOUWT COALITIES VOOR VRIJHEID, VEILIGHEID EN VREDE IN HET CYBERDOMEIN

Nederland is gebaat bij een stabiel, vrij en toegankelijk cyberdomein en wil daarom een voortrekkersrol blijven innemen in de bescherming van dit domein. Met Den Haag als internationale stad voor vrede en recht zal Nederland zich inzetten voor het in multi-stakeholder verband ontwikkelen van normen en standaarden en de bescherming van fundamentele rechten en waarden in cyberspace. Daarnaast zal Nederland zich met internationale partners inzetten om conflicten in het cyberdomein te voorkomen en te beslechten. Effectief reageren op deze conflicten beperkt zich niet tot enkel het cyberdomein, maar vraagt net als andere veiligheidsdreigingen om een geïntegreerde benadering. Inzet van traditionele elementen zoals diplomatie, inzet van sancties, capaciteitsopbouw en Defensiecapaciteiten moeten worden aangepast aan het specifieke karakter van het cyberdomein. Hiertoe worden cybercapaciteiten ontwikkeld die passen in de 3D-benadering (Development, Diplomacy, Defense).

8 Cyberdiplomatie: kennisknooppunt voor conflictpreventie

Nederland zet in op de ontwikkeling van een kennisknooppunt op het gebied van internationaal recht en cybersecurity met als doel het bevorderen van het vreedzaam gebruik van het cyberdomein. Hiertoe verbindt Nederland kennis vanuit bestaande centra. Binnen het knooppunt worden internationale experts en beleidsmakers, diplomaten, militairen en NGO's samengebracht. Zo wordt een netwerk gevormd dat de multidisciplinaire kennis samenbrengt over onderwerpen als internationale standaarden en normen voor conflictpreventie, civiel-militaire samenwerking en non-proliferatie van cyberwapens. Ook draagt het netwerk bij aan de discussie daarover. Dit is de basis voor een reeks multi-stakeholder high-level bijeenkomsten.

3.6 NEDERLAND BESCHIKT OVER VOLDOENDE CYBERSECURITYKENNIS EN -KUNDE EN INVESTEERT IN ICT-INNOVATIE OM ONZE CYBERSECURITYDOELSTELLINGEN TE HALEN

Cybersecurity heeft tot nu toe een relatief bescheiden plek binnen het onderwijs. Bekwame gebruikers en voldoende cybersecurityprofessionals zijn noodzakelijk om optimaal gebruik te maken van de kansen die digitalisering ons biedt en weerbaar te zijn tegen de steeds

25 Binnen de Nederlandse overheid bevorderen Forum en College Standaardisatie interoperabiliteit en de toepassing van open standaarden middels een lijst met aanbevolen en verplichte standaarden die gelden voor de (semi-)publieke sector.

geavanceerdere dreigingen. Cybersecurityprofessionals zijn daarnaast hard nodig om de cybersecurity-oplossingen voor de toekomst te ontwerpen en te bouwen. Nederland zit vol met ICT-talent. Dat moet echter al op de middelbare school worden aangeboord en doorstromen naar topopleidingen op MBO-, HBO- en wetenschappelijk niveau. Nederland kiest daarom voor een brede benadering: van basisschool tot hoger onderwijs van praktijkopleidingen tot universiteit, in de boardroom en op de werkvloer. Naast onderwijs en opleidingen blijven ook voorlichtingscampagnes van belang. Om de stap van bewust naar bekwaam te zetten zullen deze campagnes gerichter worden ingezet en meer aandacht geven aan het handelingsperspectief van de doelgroep.

Een excellente cybersecurity-kennisinfrastructuur ondersteunt niet alleen de weerbaarheid van onze samenleving, maar biedt ook kansen voor het ontwikkelen van expertise en het vinden van niches. Hiervoor moet een aantrekkelijk onderzoeks- en onderwijsklimaat worden gecreëerd waarbinnen cybersecurity een prominente plek heeft. Om cybersecurity-innovatie te stimuleren is een multidisciplinaire aanpak nodig waarbij ook de niet-technische deelgebieden worden meegenomen. De innovatieve producten en diensten die zo worden ontwikkeld helpen Nederland in te spelen op de snelle (technologische) ontwikkelingen in het digitale domein. Dutch design (in security) kan daarnaast een onderscheidend kwaliteitsstempel zijn voor veiligheid en privacy in ICT-producten en -diensten en bijdragen aan economische groei.

9 Taskforce cybersecurity onderwijs
Om de pool van cybersecurity-experts te vergroten en de cybersecurityvaardigheden van gebruikers te versterken, slaan bedrijfsleven en overheid de handen ineen voor een beter aanbod van ICT-onderwijs binnen zowel het lager, hoger als professioneel onderwijs. Er zal een PPS-taskforce Cybersecurity Onderwijs worden ingesteld die zich richt op advisering over het cybersecurity-onderwijsaanbod. De taskforce richt zich onder meer op certificering en diplomering van informatiebeveiligers en het (verder) ontwikkelen van lesmodules. Voor cybersecurity wordt vooralsnog aansluiting gezocht bij lopende initiatieven rond informatica-onderwijs en het Techniekpact.

10 Stimuleren van innovatie in cybersecurity
De technologische ontwikkelingen in het digitale domein gaan snel. Om daarop te kunnen anticiperen, is innovatiebeleid cruciaal. Innovatie ontstaat daar waar creatieve en kundige mensen elkaar ontmoeten. Dat alleen is echter niet voldoende. Meer coördinatie op vraag en aanbod is gewenst. Dit wordt bereikt door bestaande innovatie-initiatieven[26] en het topsectorenbeleid aan elkaar te verbinden. Daarnaast zullen overheid, bedrijfsleven en wetenschap een cybersecurityplatform lanceren. Daar kunnen gevestigde bedrijven, studenten en onderzoekers elkaar vinden, inspireren en onderzoeksvraag en -aanbod op elkaar afstemmen. De overheid levert hieraan een bijdrage met het organiseren van een vervolg op het SBIR-onderzoeksprogramma uit 2012-2013. Ook het in PPS-verband verder uitvoeren van de (tweede editie van de) Nationale Cyber Security Research Agenda (NCSRA) draagt hieraan bij.

3.7 EEN GEZAMENLIJKE INSPANNING
De ambitie van de regering en Nederland op het terrein van cybersecurity is groot en omvat een bredere meerjarige visie. Deze ambitie weerspiegelt het belang en de kansen van ICT voor onze samenleving en onze economie, evenals de huidige dreigingen en risico's. Een gezamenlijke inspanning van alle betrokkenen is hiervoor nodig, waarbij eenieder zijn eigen verantwoordelijkheid moet nemen. Daarom heeft de regering bij de totstandkoming van de strategie vele betrokken organisaties uit overheid en bedrijfsleven uitgenodigd mee te denken. De financiële mogelijkheden zijn door de huidige economische situatie beperkt.

De meerjarige ambitie is in deze strategie voor de jaren 2014-2016 concreet vertaald in het actieprogramma 2014-2016 (zie ook bijlage 1). Dit actieprogramma wordt vormgegeven binnen datgene wat reeds in de reguliere begrotingen van de departementen en partners is opgenomen. Geheel in lijn met de beweging die met het actieprogramma wordt ingezet, zal door participatie, herprioritering, smart coalitions en een geïntegreerde aanpak uitvoering worden gegeven aan de bredere strategie, die inspeelt op een toenemende problematiek die onze welvaart en welzijn bedreigt. Het weergeven van de meerjarige ambitie toont daarnaast dat het realiseren van een ook op de lange termijn veilig cyberdomein niet vrijblijvend is. Deze ambitie krijgt nader vorm in toekomstige actieprogramma's en zal moeten worden gedekt binnen de dan geldende financiële kaders. Voor de uitvoering van de actieprogramma's is commitment en samenwerking met (markt)partijen onontbeerlijk. De nadere uitwerking dan wel uitvoering van de in de bijlage genoemde acties vindt daarom plaats in overleg en/of samenwerking met private partijen en betrokken overheden.

26 Zoals de Nationale Cyber Security Research Agenda (NCSRA) en The Hague Security Delta (HSD).

Bijlage 1: Actieprogramma 2014-2016



Doelstelling 1:

Nederland is weerbaar tegen cyberaanvallen en beschermt zijn vitale belangen in het digitale domein

Actie	Wie[27]	Wanneer
1. Cybersecurity wordt opgenomen in de aanpak vitale infrastructuur. Onderdeel daarvan is een periodiek beeld van welke ICT afhankelijke systemen, diensten en processen vitaal zijn. Hieraan gekoppeld een weerbaarheidverhogend programma en publiek private crisisoefeningen.	In overleg met vakdepartementen, vitale sectoren (waaronder medeoverheden)	2014 en verder
2. Ontwikkelen van stelsel van gedragen open (technische) standaarden en minimumeisen voor het vergroten van de digitale veiligheid van vitale processen. Daarbij wordt waar mogelijk aangesloten bij bestaande (internationale) standaarden en best practices.	Vakdepartementen, NCSC Vitale sectoren	2014
3. Stimuleren van privacy en security by design in de aanbestedingstrajecten van producten en diensten voor de overheid.	Alle ministeries	2014-2016
4. Uitvoeren van een verkenning naar een gescheiden ICT-netwerk voor (publieke en private) vitale processen.	VenJ, vakdepartementen	2014
5. Op- en uitbouwen van een Nationaal Detectie- en Responsnetwerk.	VenJ, BZK, Defensie, publieke en private samenwerkingspartners	2013 en verder
6. Digitale weerbaarheid van de Nederlandse defensiesystemen versterken en het vermogen vergroten om cyber operations uit te voeren.	Defensie	2014-2015
7. Lokale overheden committeren aan een versterkte aanpak van informatieveiligheid.	BZK (Taskforce BID)	2014
8. Benoemen van verantwoordelijkheden en vastleggen van procedures (waaronder opschaling) in geval van organisatie-overstijgende incidenten die geen crisis zijn.	BZK, VenJ, I&V-diensten, medeoverheden	2015
9. Versterken onderzoeks- en analysecapaciteit om inzicht te krijgen in dreigingen en risico's in het cyberdomein.	I&V-diensten, NCSC, politie	2014
10. Versterking van het NCSC, onder andere door verbreding naar Cyber Security Operations Center, naast zijn rol van CERT.	NCSC, I&V-diensten, vitale sectoren	2014

27 Met inachtneming van bestaande verantwoordelijkheden.

11. Risico's in kaart brengen van legacy systemen in vitale processen en diensten.	VenJ, BZK	2014
12. Versterking bestaande sectorale toezichthouders door opnemen cybersecurity vereisten (waarbij overlap/dubbeling dient te worden voorkomen).	sectorale toezichthouders en vakdepartementen	2015
13. Verkennen mogelijkheid tot accrediteren van bedrijven die als 'digitale brandweer' ingeschakeld kunnen worden.	VenJ/NCSC en vitale sectoren	2015
14. Oprichten cyberreservistenbestand.	Defensie	2013
15. Oprichten Defensie Cyber Commando ten behoeve van algehele coördinatie en afstemming en gereedstelling van cybercapaciteiten.	Defensie	2014

Doelstelling 2:
Nederland pakt cybercrime aan

Actie	Wie	Wanneer
16. Actualisatie en versterking (inter)nationale (straf)wetgeving (onder andere de Wet Computercriminaliteit III).	VenJ	2014-2016 (WCIII 2014 afgerond)
17. Verbetering samenwerking met EC3 van Europol, onder andere door uitwisseling van kennis en personeel.	VenJ	2014-2016
18. Versterking van opsporing en vervolging van cybercrime als onderwerp meegenomen in discussie nieuwe Landelijke Prioriteiten (de huidige lopen tot 1 januari 2015).	VenJ, OM en Politie	2014
19. Versterking bestrijding cybercrime in de financiële sector door middel van samenwerking.	VenJ, DNB, OM, Politie, FIOD, NVB, Bancaire sector breed	2014
20. Aantal internationale onderzoeken wordt uitgebreid tot 20 in 2014.	VenJ, OM, burgemeesters en politie	2014
21. Toezien op aansluiting van de opsporing- en vervolgings-diensten bij digitalisering van criminaliteit.	Inspectie VenJ	2014
22. Versterking van het intake- en registratieproces van aangiften cybercrime bij de politie.	Politie	2014-2016

Doelstelling 3:

Nederland investeert in veilige en privacy bevorderende ICT producten en diensten

Actie	Wie	Wanneer
23. Verbeteren en of ontwikkelen van standaarden, zoveel mogelijk in internationaal verband, die gebruikt worden om veiligheid en privacy van ICT- producten en -diensten te bevorderen.	Vakdepartementen en samenwerkingspartners	2014 en verder
24. Lanceren van bewustzijnscampagnes zoals Alert Online, waarbij privacy ook onderdeel is.	VenJ, CBP, ECP	2014-2016

Doelstelling 4

Nederland bouwt coalities voor vrijheid, veiligheid en vrede in het digitale domein

Actie	Wie	Wanneer
25. Vormgeven van cyberdiplomatie en samen met internationale partners ontwikkelen van normen en vertrouwenwekkende maatregelen om conflictescalatie in het digitale domein tegen te gaan.	BuZa, VenJ	2014-2016
26. Het ontwikkelen van een kennisknooppunt op het gebied van internationaal recht en cybersecurity met als doel het bevorderen van conflictpreventie in het cyberdomein. Daartoe wordt onder andere een serie high level bijeenkomsten georganiseerd.	BuZa, VenJ	2014-2015
27. Internationaal voortouw blijven nemen op het terrein van internetvrijheid, onder andere met de Freedom Online Coalition (FOC), en inzetten op een krachtige Europese aanpak van privacybescherming en fundamentele rechten en waarden vis-à-vis derde landen.	BuZa, BZK, VenJ	2014 en verder
28. De Nederlandse overheid zal versterkt participeren in multi-stakeholder evenementen zoals de Cyberspace Conferenties en het IGF.	EZ, BuZa, VenJ	2014
29. Nederland zet in op capaciteitsontwikkeling in derde landen op het gebied van cybersecurity via bilaterale of regionale initiatieven.	BuZa, Defensie, VenJ	2014-2016
30. Uitwerken mogelijkheden voor de nationale inzet van de digitale capaciteiten van Defensie op verzoek van civiele autoriteiten.	Defensie	2014

Doelstelling 5:

Nederland beschikt over voldoende cybersecuritykennis en -kunde en investeert in ICT-innovatie om onze cybersecuritydoelstellingen te behalen

Actie	Wie	Wanneer
31. Er zal een PPS taskforce Cybersecurity Onderwijs worden ingesteld, die zich richt op advisering over het cybersecurity onderwijsaanbod. Onder andere certificering, diplomering en het (verder) ontwikkelen van lesmodules.	VenJ, EZ, OCW	2014
32. Voor cybersecurity wordt vooralsnog aansluiting gezocht bij lopende initiatieven rond informaticaonderwijs en het Techniekpact.	OCW	2015
33. Meer stageplekken en technische *traineeships* in cybersecurity realiseren in de publieke sector.	VenJ en BZK	2015
34. AgentschapNL en NWO zullen, in vervolg op de 2012-2013 tender, opnieuw tenders uitschrijven ter waarde van ongeveer € 6 miljoen, ongeveer gelijk verdeeld over een SBIR programma en lange termijn onderzoek.	EZ, NWO (medefinanciering door vakdepartementen)	2014-2015
35. Ontwikkelen Cyber Defensie opleidings- en trainingstraject met private partijen en Regionale Opleidingscentra (ROC's).	Defensie	2014
36. Plan opstellen voor betere aansluiting op onderzoeksbehoefte in bedrijfsleven via onder andere 'scientist on the job'.	NWO/TNO i.s.m. bedrijfsleven	2013, 2014
37. Lanceren van cybersecurity platform voor nieuwe en gevestigde bedrijven, studenten en onderzoekers.	EZ, VenJ en bedrijfsleven	2015

Dit is een uitgave van de Nationaal Coördinator Terrorismebestrijding en Veiligheid

Bezoekadres
Turfmarkt 147
2511 DP Den Haag

Postadres
Postbus 20301
2500 EH Den Haag

T (070) 751 50 50
E info@nctv.minvenj.nl
I www.nctv.nl